Connecting Networks 6.0 - Chapter 5 Skills Integration Challenge

Chapter 5 SIC: Access Control List and SNMP Configuration Answers

CCNA 4 Exam Answers

A few things to keep in mind while completing this activity:

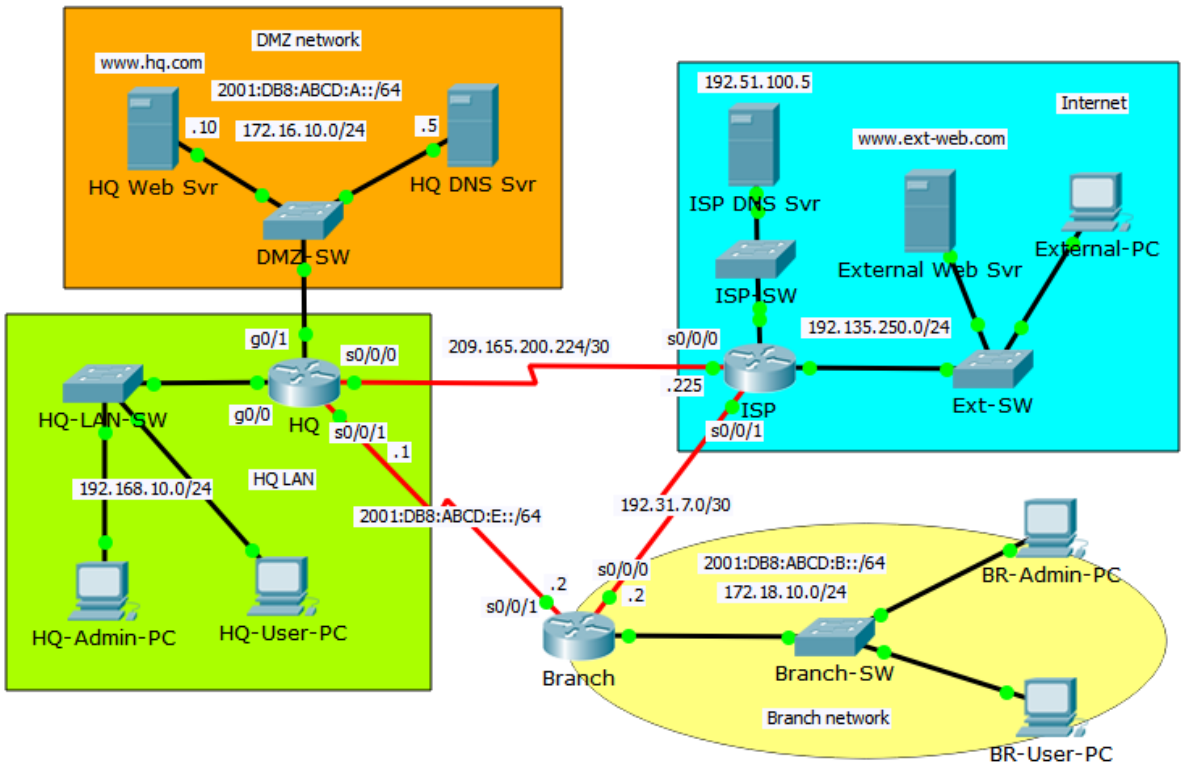
1. Do not use the browser **Back** button or close or reload any Exam windows during the exam.
2. Do not close Packet Tracer when you are done. It will close automatically.
3. Click the **Submit Assessment** button to submit your work.

Introduction

In this practice Packet Tracer Skills Based Assessment, you will:

- Configure SNMP community strings.
- Configure standard and extended IPv4 ACLs to filter network traffic.
- Configure an IPv6 ACLs to filter network traffic.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
ISP	S0/0/0	209.165.200.225	255.255.255.252	N/A
	S0/0/1	192.31.7.1	255.255.255. 252	N/A
	G0/0	192.135.250.1	255.255.255. 0	N/A
	G0/1	192.51.100.1	255.255.255. 0	
[[R1Name]]	S0/0/0	209.165.200.226	255.255.255.252	N/A
	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	172.16.10.1	255.255.255.0	N/A
		2001:DB8:ABCD:A::1/64 Link Local: FE80::1		N/A
	S0/0/1	2001:DB8:ABCD:E::1/64 Link Local: FE80::1		N/A
[[R2Name]]	S0/0/1	2001:DB8:ABCD:E::2/64 Link Local: FE80::2		N/A
	S0/0/0	192.31.7.2	255.255.255.252	N/A
	G0/0	172.18.10.1	255.255.255.0	
		2001:DB8:ABCD:B::1/64 Link Local: FE80::2		N/A
ISP DNS Svr	NIC	192.51.100.5	255.255.255.0	192.51.100.1
Ext. Web Svr	NIC	192.135.250.10	255.255.255.0	192.135.250.1
External-PC	NIC	192.135.250.5	255.255.255.0	192.135.250.1
[[DMZWName]]	NIC	172.16.10.10	255.255.255.0	172.16.10.1
		2001:DB8:ABCD:A::10/64		FE80::1
[[DMZDName]]	NIC	172.16.10.5	255.255.255.0	172.16.10.1
		2001:DB8:ABCD:A::5/64		FE80::1
[[LANAdminName]]	NIC	192.168.10.5	255.255.255.0	192.168.10.1
[[LANUserName]]	NIC	192.168.10.11	255.255.255.0	192.168.10.1
[[BRAdminName]]	NIC	172.18.10.5	255.255.255.0	172.18.10.1
		2001:DB8:ABCD:B::5/64		FE80::2
[[BRuserName]]	NIC	172.18.10.10	255.255.255.0	172.18.10.1
		2001:DB8:ABCD:B::10/64		FE80::2

Step 1: Configure SNMP Community Strings on the [[R1Name]] router.

a. Configure a Read Only SNMP community string **hq-monitor**.
b. Configure a Read/Write SNMP community string **hq-inside**.

Step 2: Configure an ACL for NAT on the [[R1Name]] router.

a. Configure standard access list numbered 1 to allow NAT for hosts in network 192.168.10.0 /24.

Step 3: Configure a standard ACL to restrict remote access to the [[R1Name]] router.

a. Configure a standard ACL numbered 12 to restrict remote access to [[R1Name]].

- Allow only the [[LANAdminName]] to access the [[R1Name]] router remotely via VTY.
- All other remote connections should fail.

Step 4: Configure two extended ACLs to restrict access to SNMP operation on the [[R1Name]] router.

a. Configure an extended ACL named SNMPACCESS.

- The SNMP operation runs UDP on port 161.
- Allow only the [[LANAdminName]] to access the [[R1Name]] router for the SNMP connection.
- SNMP connections from other hosts on the [[LANName]] should fail.
- Allow all other IP traffic.
- Apply this ACL on the [[R1Name]] router, G0/0 interface.

b. Configure an extended ACL named SNMPDENY.

- Deny any hosts to make connections to SNMP on the [[R1Name]] router.
- Allow all other IP traffic.
- Apply this ACL on the [[R1Name]] router, G0/1 interface.

Step 5: Configure an extended ACL to restrict access to the [[LANName]] from the Internet.

a. Configure an extended IPv4 ACL named INTOHQ.

- Allow any hosts from the Internet to access the [[DMZDName]]. There should be two ACEs, one for TCP and the other UDP. Both use port 53.
- Allow any hosts from the Internet to access the [[DMZWName]]. Only port 80 is needed.
- Allow return TCP traffic from the Internet that was initiated from the hosts in the [[R1Name]] networks to pass (with the **established** keyword).
- Apply the ACL to the [[R1Name]] S0/0/0 interface.

Step 6: Configure an extended ACL to restrict access to the DMZ network.

a. Configure an extended IPv4 ACL named IN-DMZ.

- Allow any hosts to access the [[DMZDName]]. There should be two ACEs, one for TCP and the other UDP. Both use port 53.
- Allow any hosts to access the [[DMZWName]]. Only port 80 is needed.
- Allow only the [[LANAdminName]] to have FTP access to the [[DMZWName]]. There should be two ACEs, for ports 20 and 21.
- Apply the ACL to the [[R1Name]] G0/1 interface.

Step 7: Configure an IPv6 ACL to restrict access to the DMZ network from the [[BRLName]]. (*Please note, the order of ACL statements is significant only because of the scoring need in Packet Tracer*).

a. Configure an IPv6 ACL named DMZFTP.

- Deny any hosts in the Branch network to access the SNMP operation of the [[R1Name]] router.
- Allow only [[BRAdminName]] to have FTP access to the [[DMZWName]]. There should be two ACEs, for ports 20 and 21.
- Allow any hosts in the [[BRLName]] to access the [[DMZWName]]. Only port 80 is needed.
- Apply the ACL to the [[R1Name]] router S0/0/1 interface.

Step 8: Connectivity Tests

a. [[LANAdminName]] can access FTP service on [[DMZWName]].
b. [[LANUserName]] cannot access FTP service on [[DMZWName]].
c. [[BRAdminName]] can access FTP service on [[DMZWName]] with its IPv6 address.
d. [[BRuserName]] cannot access FTP service on [[DMZWName]] with its IPv6 address.
e. [[LANAdminName]], [[LANUserName]], and External-PC can access [[DMZWName]] with URL **www.hq.com**
f. [[LANAdminName]], [[LANUserName]], and External-PC can access External Web Srv with URL **www.ext-web.com**
g. [[BRAdminName]] and [[BRuserName]] can access [[DMZWName]] with its IPv6 address
h. [[BRAdminName]] and [[BRuserName]] can access External Web Srv with URL **www.ext-web.com**

Last Updated: December, 2016

ID:[[nameindex]]

Version 1.0
Created in Packet Tracer 6.3.0.0009 and PT Marvel 2.0.5